(2½ Hours) **[Total Marks: 75]**

N.B. 1) **All** questions are **compulsory.**
2) **Figures** to the **right** indicate marks.
3) **Illustrations**, in-depth answers and diagrams will be appreciated.
4) **Mixing** of sub-questions is **not allowed.**

Q. 1 Attempt Allthe Questions **(15M)**

(a) Multiple Choice Questions:

1. Programs designed to affect performance and not damage the system are called
   a) BOT's b) Spyware
   c) Virus d) Worm
2. Which one of the following is not a part of Metasploit interface
   a) msfgui b) msfconsole
   c) msfconsole d) msfpayload
3. What is the first step in a SQL injection attack?
   a) Enter arbitrary commands at a user prompt b) Locate a user field on a web page
   c) Locate the return pointer d) Enter a series of NOPs
4. What type of device connects systems on a shared network?
   a) Routers b) Gateways
   c) Hubs d) Switches
5. Entering **Password::blah** or **1=1** into a web form in order to get a password is an example of what type of attack?
   a) Buffer overflow b) Heap-based overflow
   c) Stack-based overflow d) SQL injection

(b) Fill in the blanks (Use following pool to answer questions)

[DNS poisoning, Session ID, passive, Sequence number, MAC, SYN, active, BOT]

1. A_____ indicates where the packet is located in the data stream so the receiving station can reassemble the data.
2. In a _____ attack, an attacker hijacks a session and then watches and records all the traffic that is being sent by the legitimate user.
3. A _____ flood attack sends TCP connection requests faster than a machine can process.
4. A _____ is an automated software program that behaves intelligently.
5. _____ is a technique that tricks a DNS server into believing it has received authentic information when in reality it has not.

(c) Answer in ONE or TWO sentences:

1. Name any three threats in information security.
2. List different ways to detect DoS attacks.
3. What is session hijacking?
4. What are two types of buffer overflow attacks?
5. Mention any two VOIP Vulnerabilities.

Q. 2 Attempt the following (Any THREE) (15M)

(a) Explain the following terms:
a. Keystroke Logging
b. Denial of Service (DoS /DDoS)

(b) Explain the statement "As Security increases system's functions and ease of use decreases for users".

(c) Define a Worm and Virus. Mention the differences between the two.

(d) Explain ARP poisoning in detail

(e) What are BOTs and BOTNETs? Explain.

(f) What is an attack? Explain in brief rootkit attack.

Q. 3 Attempt the following (Any THREE) (15M)

(a) What is Footprinting? What countermeasures can be taken against footprinting?

(b) Write a short note on phases of hacking.

(c) Explain the need for repeated penetration testing.

(d) Describe the implementation of Request Forging using XSRF/CSRF.

(e) Explain Authenticated and Unauthenticated Penetration Testing.

(f) Describe the several steps involved in Security testing plan.

Q. 4 Attempt the following (Any THREE) (15M)

(a) Write a note on Covering your tracks phase.

(b) What is password cracking? Explain various steps involved in cracking a password.

(c) Write a short note on SYN flooding.

(d) Describe in detail SMTP/Email based attack.

(e) Explain the different steps adopted to secure a VOIP Network.

(f) Explain Honeypots and different evasion technique.

Q. 5 Attempt the following (Any THREE) (15M)

(a) Explain in brief DNS poisoning.

(b) Describe threat modelling.

(c) Explain internal and external penetration testing with suitable example.

(d) Write a short note on cross site scripting (XSS).

(e) Explain Metasploit in detail using Kali Linux.
